Thank you for sharing, Edward. Ransomware is a type of malware attack aimed to limit users’ access to a computer or encrypt users’ files spread through exploit kits and phishing techniques, impacting the availability of data until a ransom is paid. Ransomware is on a dangerous rise expected to result in $20 billion in yearly damages in 2021, an approximately 174% increase since 2019 (Hamdan Mohammad, 2020).

The example you presented of Kaseya’s 2021 ransomware attack is particularly frightening. Small to medium size businesses with modest technical resources heavily rely on managed service providers (MSPs) for information technology support and services. By working with an MSP, businesses that cannot otherwise afford a robust IT department and infrastructure still receive the benefits of an MSP’s staff expertise and system resources. Depending on the subscription and support model, an MSP can have access to multiple clients’ network and user systems, making it an attractive target to threat actors. Compromising an MSP environment can result in impacting several MSP customers, allowing the attacker to demand the MSP or the individual customers for ransom. In addition to the monetary loss incurred by the MSP and customers, both parties’ risk reputational damage. MSPs need to implement appropriate detective and preventative technical and administrative controls to protect against ransomware attacks. Such controls include file activity and event tracing through auditing, honeypots/honeynets, cybersecurity awareness training, antivirus, and machine learning technologies like anomaly-based firewalls (Hamdan Mohammad, 2020).

Working with an MSP is a way of mitigating cyber risk, however businesses need to ensure the MSP offers strong assurance when it comes to security. Businesses can request an MSP to provide Service Organization Control (SOC) 2 audit reports to understand how a service provider protects client data, assets, and privacy hence protecting against potential attacks like ransomware (SOC 2® Examination That Addresses Additional Subject Matters and Additional Criteria, n.d.).

**Reference List**

Hamdan Mohammad, A., 2020. *Ransomware Evolution, Growth and Recommendation for Detection*. [online] Available at: <https://www.researchgate.net/profile/Adel-Mohammad-2/publication/339511130\_Ransomware\_Evolution\_Growth\_and\_Recommendation\_for\_Detection/links/5ea35350299bf112560c2360/Ransomware-Evolution-Growth-and-Recommendation-for-Detection.pdf> [Accessed 29 August 2021].

  AICPA. n.d. *SOC 2® Examination That Addresses Additional Subject Matters and Additional Criteria*. [online] Available at: <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/soc2additionalsubjectmatter.html> [Accessed 29 August 2021].